Security Culture: Building a Better Mindset to Withstand the Digital Threat Landscape

Introduction

In sports you'll often hear fans and coaches say the same thing: the best offense is a good defense.

In Information Technology the best defense is obsessive paranoia.

Welcome to the wonderful world of Information Security (also known as Cyber Security and, for the rest of this book, InfoSec).

InfoSec is a constant race between you and the smartest, best-funded, most advanced attackers in history.

If it sounds daunting that's because it is. Maintaining security in the modern technological landscape can sometimes feel like trying to shore up a sandcastle against the tide. You put up one defense and it's cracked a week later; you implement a solution and a month down the line an exploit is revealed and your solution is useless.

But that's no reason to throw up your hands and give up hope – it's an invitation to change your way of thinking. What you need to have good security in the modern threat landscape isn't the newest and best innovation – what you need is to build a culture of security in yourself and your environment.

Let's start with the basics.

Why should you care about information security?

At its core the importance of InfoSec rests on three simple principles:

- Confidentiality
- Integrity
- Availability

This is known as the "CIA Triad" or "Security Triad."

Security exists to keep your information private, un-tampered-with, and easily accessible.

In other words: InfoSec matters because it's the foundation you need to trust your data.

If we consider something along the lines of a traditional piece of postal mail we can see this trust in its simplest form. Confidentiality – the envelope that keeps the contents of a letter secret; Integrity – the seal of the envelope, which shows the recipient that nobody has opened it and added or changed information; Availability – information that can be accessed in a couple of easy steps like going to the mailbox and opening an envelope.

A piece of mail, for all that it is an old technology, displays the principles of Information Security soundly.

Of course, letters *are* an old technology. Envelopes are no guarantee of privacy and sticky glue seals can be opened with a teakettle.

The world has moved beyond believing in the sanctity of the mail.

Now confidentiality is why we put our faith in passwords and encryption, firewalls and antiviruses shore up the integrity of our information, and cloud storage has become the big innovation in availability.

But encryption can be cracked, firewalls can be exploited, and you can lose access to the cloud if the internet goes down.

Relying on individual technologies, though they may be new and strong when they are introduced, is not the way to protect your information.

Again, you need to build a culture of security.

What Makes a Culture of Security

In this book you will be introduced to some of the main systems threatened by InfoSec attacks and throughout you will be asked to not only consider the technologies that can improve their security but also to consider what behaviors you can implement that can improve the security of your environment.

There's a quote from Benjamin Franklin that a lot of hackers like: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." (1)

Hackers have adapted the statement to the realities of a security culture: "Those who would give up security for convenience deserve neither."

In the last ten years the balance of Confidentiality/Integrity/Accessibility has shifted too far in the direction of Accessibility (convenience).

People want all their accounts synced to one password, they want all of their information accessible on one device, they want their face to unlock their phone and their phone to unlock their house.

This is convenience at the expense of integrity and confidentiality.

A culture of security is understanding the need to balance these principles, but it is also the recognition that you have to learn to be a pessimist.

A security culture is asking "What's the worst thing that could happen," answering that question honestly, and preparing for that eventuality.

Whereas a culture of convenience might say "we should keep our backups local so they're always accessible when we need them" a culture of security would say "local backups are nice to have but we should also have a cloud backup in case the building catches fire and we should also have an archival backup in case the building catches fire and solar storms take down the internet."

A culture of convenience says "I love how easy it is to use my face to lock my phone, it lets me keep things private without having to remember a password" a culture of security says "if I use my face to unlock my phone anyone who is willing to steal my phone and take a picture of me has access to all of the information on my phone."

A culture of security is always, always keeping in mind that there are a hundred people in the world today who could crack through your toughest encryption tomorrow, so you've got to plan for the day after that.

A culture of security is knowing that things will never be perfect, but that doesn't mean they can't be good.

Getting Good

There is a certain nihilism that comes from spending a long time getting familiar with security. At a certain point you simply have to recognize that if the Queen of England wants your data she has the resources to break through almost any security you could enact to prevent that from happening.

But that doesn't mean you need to make it easy for her.

Sometimes good security is as simple as frustrating your attackers enough times that they give up, or blocking their attacks just long enough that you can run one more full backup.

Good security doesn't mean your systems are invincible, they mean that your can be reasonably sure that your data is kept confidential, that it hasn't been tampered with, and that you can use it when you need it. Good security is about building a foundation of trust.

This book exists to tell you some of the ways that you can make that happen.

Chapter 1 – If You Have a Good Backup You Don't Need the Rest of this Book

In the spring of 2019 the City of Baltimore learned a hard lesson about backups. A ransomware attack on the city's servers taught the local government IT department that a good backup isn't exactly priceless – it's worth at least $18.2 million (1).

Ransomware infected the city's network, traveling from computer to computer and encrypting the hard drives of individual desktops as well as the city's servers, and within hours all of the data for the City of Baltimore was being held hostage (2). The infection took down city phone lines, killed off payment systems, and put the business of Baltimore in a state of limbo. It also revealed one remarkable mistake that could have prevented all of this: instead of being backed up to a local server and rotating drives or being backed up remotely to cloud storage most of the city data was stored on individual user workstations (3).

There are two main types of backups, file backups and image backups. File backups store the files on a computer, image backups store a snapshot of all the computer's programs, settings, and files at the time the backup was made.

If the City of Baltimore had made image backups of their servers or kept file backups of employee desktops it could have saved the city millions of dollars, if not the entire cost of the system repairs and revenue lost to downtime.

If the city had good backups then restoring functionality would have been a few weeks' worth of frustrating installations and a harried IT staff. As things happened data were permanently lost, some systems were down from May until September, and the city IT Director resigned once it came to light that his office hadn't met even the bare minimum standards in protecting Baltimore's IT infrastructure.

And this isn't a new, unprecedented threat. In June 2017 a Honda plant in Japan was shut down by a virus attack that locked users out of their computers (4). In September of the same year a Dutch subsidiary of international shipping giant FedEx was infected with ransomware that locked down infected computers, costing the company $300 million in lost productivity (5).

Clearly more people needed to learn this lesson after Baltimore as well – in June 2019 Norsk Hydro, one of the world's largest aluminum producers, was infected with WannaCry ransomware and lost over $50 million and three months productivity (6)

Backups are the single easiest, cheapest, and best way to protect yourself from a catastrophic loss of data and productivity.

What is a Backup?

A backup is a copy of your data. It can be a full copy of your data and programs stored on another computer, it can be a copy of all the files you have on your computer stored on an external hard drive, it can be a snapshot of your computer and files stored on the cloud, it can be all of your data copied onto archival media and buried in a mountain - which is an actual backup solution used by the US government (7)!

How are Backups Made?

Backups are made in many different ways. You can create a manual backup by copying data from a computer or server to a hard drive, there are backups that can be run through programs included with an operating system (image backups tend to use integrated OS software instead of software from an outside provider), or you can use a third-party software to run a regular scheduled backup.

Manually copying your data to an external drive is a cheap solution but it's not easy and it's not foolproof. Home users might choose to do manual file backups on a regular basis to save money on a backup software subscription, professional IT departments might occasionally choose to manually back up important files and databases.

It makes a lot of sense to do a manual backup of important files before you make changes to your computer so that if something goes catastrophically wrong while changes are made you have a very recent copy of the data that was on your device.

If an IT company wanted to migrate a database from an old server to a new server, or if they wanted to install a new OS on a database server, it would be very sensible to manually copy the database file to an external drive so that the file couldn't be corrupted.

Some computer operating systems give users the option to use a program that comes with the OS – Apple's Time Machine and Microsoft's Windows Backup are two examples of a backup program included with the operating system. Windows Server Backup is an example of an OS-based backup solution that works for server-level devices.

There are, however, problems with OS backup solutions. Frequently they are less flexible than paid software solutions and users may find them difficult to fine-tune to their preferences.

There are many software vendors who create third-party backup solutions; these programs include products like Carbonite, Acronis, and Veeam.

Microsoft OneDrive and Apple's iCloud are cloud backup solutions that have a free tier for small amounts of storage and a monthly price for storage above that limit.

The advantage of using a software or cloud solution over manual backups is that the backup is scheduled for you based on your specifications. You can tell the software only to backup previously unsaved files; you can ask it to back up daily or on every third Thursday; you can tell it to only back up one specific location on your computer; you can do all of that and you don't have to remember to do anything except maybe to plug in your external storage drive. Some cloud backups go even further than automatically backing up on a schedule and instead they store all changes all the time – any change a user makes to their iPhone, for instance, is immediately saved to their iCloud.

Local Vs. Cloud Vs. Archival

- **Local Backups**

Local backups are hard disk backups that you store locally. The are inexpensive and extremely convenient.

Hard drive prices have fallen tremendously in the last few years so there is absolutely no reason that you shouldn't at least have a local backup of your computer or your data copied onto an external drive. As of this writing (July 2020) it's possible to purchase a 5TB storage drive the size of a small paperback

book for around $120.00 and it's a matter of a couple of hours to do an image backup of a device with a few terabytes stored on it.

This is an extremely simple blunt instrument that nonetheless can be the difference between millions of dollars and hundreds of hours lost or a few hours waiting for the server to restore from an image.

However, if all of your backups are local backups you're putting yourself at risk, and there are a few considerations you need to keep in mind:

1. If your local backup drive is plugged into your computer or server and the computer or server is infected with viruses or malware then your backup drive is also infected with viruses or malware. To prevent this tech experts recommend that you unplug your drive as soon as the most recent backup has run. Our advice is the use of three drives – a stationary drive that gets a backup every night and stays plugged into the server and two daily rotating drives that get switched out every other day. This setup means that in the absolute worst-case scenario (your server gets infected and infects the stationary drive and the rotating drive before the rotating drive has been unplugged) you've got one backup ready to go that is no more than one day old.
2. Local backups either need to be encrypted or protected in a secured location and encrypted is better. An unencrypted local backup has all of the data you store on your devices ready to be read by anyone who can plug the drive into another computer. If one of these drives makes its way out of your office or gets lost that opens you up to significant liability and can be a personal threat for identity theft if you're backing up a home computer.
3. If something knocks out your server it will probably also knock out your local backup drive. The classic example of this is a backup drive and a server that are stored in the same building and lost to a fire. Having a local backup as your only backup does you absolutely no good if it can be turned into a useless hunk of plastic by the server room sprinkler system.

For all of their risks it is difficult to overstate the sheer convenience of a local hard drive backup. If your server goes down because it was infected or because a hard drive dies then it is extremely simple to retrieve your files from a local drive and it is much faster to connect to a USB 3.0 device and copy data than it is to download data over an internet connection.

Local backups are an extremely useful tool to have in your security arsenal, but they shouldn't be the only backup you rely on.

- **Cloud Backups**

When people talk about storing things "on the cloud" what they mean is they are storing things "on someone else's server."

Cloud storage is the allotted space that you have reserved on a server that is not in your home or office, and therefore saves you the trouble of hosting your own backup storage and keeps your data safely offsite if, say, an earthquake knocks out all the power in Los Angeles.

Cloud backups are not perfect, though, and there are logistical concerns that need to be taken into consideration.

1. It is much more expensive to store your backups on someone else's server than it is to store them locally. While you can get 5TB of local storage for under $200 it might cost you nearly $100 a month to store a terabyte of data on Amazon's Cloud Storage (8).
2. If the internet goes down you don't have access to your backup. That's the harsh reality of cloud storage systems; they'll protect your data in an emergency, but that same emergency might make it impossible to retrieve your data.
3. "Someone else's server" also means "someone else's security" – Cloud Storage services have been hacked in the past and will be hacked again in the future (9). If you are going to use cloud storage you need to make sure to encrypt your data, which has its own downsides: decrypting data can make retrieving your data take longer and if you forget the encryption key your data is lost forever.

- **Archival Backups**

Archival backups are relatively rare. They are offsite storage of your data on archival media, meaning that they are frequently written to tape drives or archival optical media (6) instead of platter drives or flash drives. Archival backups tend to be used by groups that work with high clearance levels or who need to save blueprints or designs. Aerospace companies, governments, and in some cases law firms or accountancy firms may use archival backups.

The biggest downside of archival backups is that they are expensive, the second biggest downside is that they are relatively inaccessible. Very few archival backup providers exist these days, as it's a specialized kind of backup that is overkill for the average office or home user.

Centralization

In business environments keeping data centralized is an important part of keeping a good backup. If your employees all work on their own individual workstations and never store their work to a single location you're just increasing the chances that you're going to lose a portion of your data.

Employees should also be backing up their individual workstations but beyond that you should have a plan in place to save their work as they go.

This is one of the major advantages of server-based software like database programs or multi-user installations – the work that each employee does may be saved to their workstation but it is also stored centrally, which means that if a single employee's workstation is infected by a virus or happens to catch fire all of that employee's data is still available to them and to your company.

Backups and Security Culture

Backups are the foundational bedrock of building a solid security culture because they're the simplest, cheapest, best, and most honest way of approaching a worst-case scenario.

A good backup is the answer to the security culture question you should ask yourself every day: "What if I turn on the server this morning and instead of turning on it explodes?"

Backups are preparing for the worst eventuality. A solid backup plan should withstand the 10 Plagues of Egypt (yes, including the killing of the firstborn because you should never rely on only one person to know the encryption key for your backups).

Returning again to the example that started this chapter we can see that the IT department for the City of Baltimore was woefully lacking in a security culture. Their data wasn't centrally collected in one place, backups were irregular at best, and there was no single backup plan that included the possibility of failure in any one of its parts. Since the backups for the City of Baltimore failed in every single one of their parts this meant that the recovery effort was long, arduous, and permanently lost data that could never be recovered.

Baltimore is a warning about what happens when you don't ask yourself uncomfortable questions.

Another uncomfortable question you need to ask yourself is this: "How much would someone pay one of my employees to hand them a backup drive?"

If you aren't 100% positive that every single one of your employees would walk away from a ten million dollar payment to hand one of your backup drives to a shadowy figure in an alley you need to make sure that your backups are encrypted and that you've got security features in place that will prevent random people from decrypting the files but that *also* will allow legitimate users to access the information if the encryption key is lost.

Finding the right backup solution can sometimes feel like threading a needle, but when you've done it correctly it is the single greatest tool in your arsenal to protect against attackers and other disasters.

What You Can do to Protect Yourself Today

If you have no current backup plan there's no better place to start than by doing an image backup of your personal computer. It's simple, it's fast, it's inexpensive, and it means that if your computer is stolen by a vengeful seagull you'll be able to create an exact duplicate of your computer on another device.

Here are some simple instructions to do an image backup of your PC:

- To start you will need a USB backup drive that is at least as large as the current hard drive on your computer. To check the size of your drive go to Settings > System > Storage and look at the size of your drive.
- Plug a USB drive that is larger than your current hard drive into your computer.
- Go to Update & Security > Backup and click on "Backup and Restore (Windows 7)" (do this even if you're using Windows 10) and it will open control panel window.
- In the new window there will be an option in the upper left corner for "Create System Image." Click that option and follow the instructions.
- When it gets to the end of the image backup it will ask you if you want to create a System Repair Disc – click "yes," follow the instructions, and make sure to store your System Repair Disc and the hard drive with your Image Backup in a safe place.
- Run regular image backups (at least twice a year) and when the backup drive starts to get full delete old backups. If you're using a 4TB external drive and your computer has a 500GB hard drive you can store around 7 backups before you need to start deleting previous backups.
-

If you do nothing else beyond simply creating an image backup of your own personal desktop you are more prepared for a disaster and more secure than the IT department of the City of Baltimore was in 2019.

Questions to Ask to Start Forming A Security Culture Mindset

- What important work would I lose if my computer were to get run over by a car today?
- How much would I be willing to pay to recover the data on my hard drive? (Keep in mind that DriveSavers, the best data recovery service in the world, can almost always get your data back but their prices start at around two thousand dollars.)
- If my computer were to get run over by a car today would I lose all my wedding photos? My photos of my grandkids? The manuscript for my novel? Chatlogs between me and a friend who passed on?
- If my computer were to get run over by a car today would I have the licensing information to reinstall all the programs that I use on this computer or would I need to purchase new licenses?
- Do I visit any websites where I might be infected with ransomware or a virus?
- Do I always practice good web hygiene when opening my emails and attachments?
- Am I aware of the current vulnerabilities in my system and have those vulnerabilities been patched?

Remember that security is, to some extent, expecting the worst and preparing for it. Think very hard about the most important things you have on your computer or the most vital information stored on your server. Think about how much it would hurt to lose that information, then start thinking about how to protect it.

Recommended Solution:

We take a hybrid approach to backups to ensure that our customers are always able to rely on accessible, secure backups.

We recommend a stationary drive attached to your server to do a nightly backup, two rotating drives to do backups every other day, and we are partnered with Veeam as a Cloud Backup Solution provider. Customer data is encrypted by the customer so that it is never visible to either us or to VEEAM, and we recommend the use of password managers and company vaults to ensure that your encryption key is accessible to those who need it.

Our skilled technicians regularly monitor the health of the backups for our contract customers to make sure there are no errors or flaws in the process that might lose your valuable data and our granular approach allows us to do everything from restoring a single file an employee may have accidentally deleted to restoring a server from the ground up in the event of a catastrophic attack or emergency.

Many of our customers have been infected by ransomware over the years, but none of the customers who adhered to our recommended backup solutions has lost more than a day’s worth of data or productivity.

Chapter 2 – Email is Inherently Insecure

In 1971 Ray Tomlinson appended the SNDMSG program by enabling it to share messages on different computers on one network by using the @ to add a hostname to the name of the recipient (1).

Sending a message over a network wasn't secure then, it isn't secure now, it won't be secure in the future, and we all have to live with that.

To understand why this is true you have to know a little bit about the history of email and its intended uses.

Email, as we know it, is based on a very simple set of protocols called Simple Mail Transfer Protocols (SMTP). SMTP was defined in the early 80s and today, just as it was then, it is essentially a simple, standardized set of protocols to allow different computers to send messages to one another (2).

When SMTP was developed the Internet was so new it could barely be called nascent. Most computer networks were either academic or military, and globally there were fewer than a million people on the web who had the technological know-how and tools available to send emails to each other.

When SMTP was defined there was essentially no need for email security because the chances that someone who wanted to attack your information would also have the ability to do so were basically nil.

When viewed through the lens of history many things about the early internet are retrospectively miraculous and email is one of those things. It's based on simple, standardized protocols that have stood up to forty years of scrutiny. In spite of the fact that many carriers have started offering their own version of email all of them need to adhere to the same standardized protocols to communicate across platforms. Anyone can set up and start hosting an email server right this second using free programs that are easy to approach. (3)

Email is an incredible innovation that allows rapid communication between people all over the globe and it's virtually free to anyone who can access the internet.

Email is democratizing, email is incredible, email is literally world-changing technology.

And it's not secure, was never intended to be secure, and the simple protocols that allow it to exist were not created with security in mind.

Email is as secure as a corkboard in a university student lounge because that's essentially what it was initially intended to be.

When SMTP was initially developed the people communicating on computer networks were all part of the same small community. Sending government secrets through email wasn't a huge risk because you were the one with the government secret sending it over a government network to a recipient who was also holding a bunch of government secrets.

In fact, one of the very early accounts of a hacker breaking into government accounts started with the same hacker exploiting an EMACS mail-mover vulnerability (4). The exact problems that we were facing with email in 1986 are the problems we're looking at 34 years later.

Emails are written, stored, and usually sent as plaintext. There are dozens of attacks that can be made at multiple points of failure in which any text sent in an email is easily readable by the attacker. The root of the problem is that email was meant to be open, not secure.

How does an Email Work?

In the very simplest terms you write an email in an email client (a program like Outlook), the email is sent to your (or your email provider's) SMTP server which then verifies the address it's going to on a DNS server. The email is then sent to the recipient's SMTP server, and then to your recipient's email client.

The SMTP servers check that the message is formatted properly, the DNS server tells the SMTP servers how to route the email, the email clients translate words into data bits on one end and back from data bits into words on the other end.

Unless you are exceptionally paranoid and highly technical then essentially none of this process is in your hands.

Many Points of Failure

Another reason that email can't be trusted for secure communication is that, as a multi-step process that is not contained within your environment, there are many points of failure at which security can be compromised and which you have no control over.

- **Email Client Security**
  Outlook is a very effective, widely-used program that has decades of known exploits against it. Its popularity is part of why it is so widely attacked and studied by bad actors. While there are ways that you can help to ensure that your email client is more secure (disable macros, require frequent logins) there is no way to protect against zero-day attacks.
- **SMTP Attacks**
  IF SMTP Relay is enabled attackers can remotely access the server to observe traffic. SMTP Man in the Middle attacks can be used to strip encryption off of emails and inject malware or false information into emails.
- **DNS Hijacking**
  If the DNS server where your SMTP server verifies its routing has been hijacked emails can be sent to incorrect, unsafe addresses.

How do You Fix a Problem Like an Email?

There are two schools of thought when it comes to security and email communication.

The first school says that email security is possible through encryption – and that's not incorrect (5)! There are many encryption options available today that weren't possible twenty years ago and that do a good job of hardening emails against various attacks. If your email is encrypted on the sender side it can't be intercepted and read on any of the servers that store or transmit it until it gets to the recipient. End-to-end encryption prevents man-in-the-middle attacks, requiring a shared key means that the message isn't stored in plaintext on the email servers anywhere along the path the email takes from sender to receiver.

The problem is that once a receiver has your email how they store it and what protections they use are at their discretion and they may be less security-minded than you are.

It's an unfortunate reality that as an MSP it is very common to be contacted by clients who have allowed interlopers to access their computers, rifle through their data, and read their emails, and if they're storing your confidential data in plaintext then your data isn't confidential anymore.

The second way of thinking about email security is to reconsider what you believe is safe to send by email and to look for other, more private options to send confidential information (6).

This is a problem that can be solved partially through the use of alternative messaging systems like Signal, which places a heavy emphasis on encryption, or even through something like Microsoft Teams, which doesn't allow users to easily download conversations or message chains to their own desktops so there's more control of data from a business perspective.

But security-focused apps are only part of the equation. You have to really sit down and ask yourself some hard questions and accept that in this instance it's more important to emphasize confidentiality than accessibility for the end user.

The way to fix the security problems with emails isn't just to focus on encrypting what you can, it is to also realize that even when your emails are encrypted there is some information that simply should not be sent through email.

Privacy Decoded

Encryption is vitally important. It is also, sometimes, tragically unreliable.

In 2018 PGP (Pretty Good Privacy), the most widely adopted email encryption protocol, was revealed to have major flaws that allowed malicious attackers to decrypt encrypted emails and view them as plaintext. (7)

The vulnerability has been patched and the security and cryptographical communities have worked on alternatives to PGP and GPG (an open source encryption option that had some of the same problems) but, in spite of these attempts to fix PGP, the central problem with encryption is that it is possible to crack.

That's not to say that it's easy or common for encryption to be broken, nor is it a frequent enough problem that encryption should be written off as useless. But if you're sending a message that absolutely no one else can ever read you have to be very, very certain that the encryption you're using can never be cracked.

Dance like no one is watching, Write emails like they'll be published on the front page of the newspaper

Since there is no way to guarantee that your emails will remain private it is imperative that you learn to use email as a tool that must be handled with caution.

Email is convenient, email is accessible, email is not how to get your credit card number to a vendor or what you should use to get your social security number to a doctor's office.

This is one of those instances where a technological solution is less important than changing the way you approach the problem in the first place.

As a whole our society has decided that plaintext messaging is the best way to communicate; we send personal information through SMS messages, we write about our hopes and dreams in social media chats, we complain about our coworkers in email, and we're constantly surprised when chatlogs, screenshots, and leaked emails cause problems.

While you're attempting to build a security culture mindset this is the perfect time to start asking yourself if you really need to have all of your sensitive information written down and stored on a computer or if there is a better way to approach the problem.

Small businesses are a lot less likely to lose credit card numbers in a data breach if they don't store credit card numbers digitally. Medical offices are much less likely to expose patient identifying information like social security numbers if they don't store social security numbers (and for many doctor's offices there is no reason to store something as sensitive as a social security number when a photocopy of a drivers' license has all of the information they need to verify identity).

If you do need to share information digitally and it does need to be stored this is a good time to question whether or not the data needs to be sent or if it can be shared in some other way.

Doctor's offices, Law firms, and Accounting groups may want to invest in the infrastructure to support a client-facing portal where customers can upload information and download documents without having to host the information on outside servers so that any risk of exposure is moved from your business to the customer, who is not liable for damages if they reveal their own data.

Consider Your Risk

The solution to the problem of how to securely communicate through email isn't a simple one (again, because email was never intended to be secure) but it also is a problem with many answers.

What you need to ask is if the convenience of email is worth the risk that it exposes you to.

As always, the security culture question to ask yourself is "what's the worst that could happen?"

If a low-stakes interoffice communication about scheduling a meeting is read by someone outside of your company the worst that can happen is that they know something about your schedule that they didn't before. This is a nuisance at most, and not something to worry about.

If a private communication about finances, infidelity, communicable disease, or even something as innocuous as job-searching falls into the wrong hands it can be disastrous for your business or for you personally.

Make a Plan to Mitigate your Risk

The easiest way to prevent sensitive information from being revealed in a captured or hacked email is to institute a set of practices that prevent sensitive information from ending up in emails.

Make it a practice in your personal and professional life to keep some types of information more private

- Financial data like credit card numbers

- Personal identification numbers such as Social Security Numbers
- Sensitive medical information
- Legal or Banking information
- And most importantly Usernames and Passwords

should never be sent over email.

Consider using different programs to share information. For interoffice communication Teams or Skype may be a better option for some kinds of sensitive information; encryption-heavy programs like CryptPad or Signal may be a good choice for other kinds of sensitive information.

If you frequently need to exchange confidential information with clients or customers consider hosting a customer document portal where users can log in to access data on servers that you host and maintain so there are fewer points of ingress for attackers.

If you are forced to use email encryption make sure that you're using the best modern standard available to you. At this point PGP is once again considered reliable if certain requirements are met and address verification is required (8).

Questions to Ask to Start Forming A Security Culture Mindset

- What is the worst thing that would happen if an email I sent fell into the wrong hands?
- If I'm sending out personal information about someone else what would happen if they had a stalker and their stalker saw this information?
- Could I get fired if my boss saw this email?
- Would I lose a customer if my customer saw this email?
- What are the ways that a bad actor could access the email that I'm about to send? Could they see it through my email client? Is it possible my traffic is being watched?
- How could I prevent an attacker from seeing this email? Would encryption be enough?
- Is typing this email where I'm sitting right now secure? Can anyone read my screen? Am I on a public WiFi access point?
- What are the other ways I could get this information to the recipient?

The Recommended Solution:

While we most strongly recommend that you do not send sensitive information through email we can help you to configure secure servers, email encryption, and implement industry standard best practices that will keep your email as secure and private as possible.